

Azure Firewall

- ✓ Create Rg-italy
- ✓ Create FirewallVnet with two subnets 1.default(subnet), 2. firewall (firewall subnet) Dedicated subnet
- ✓ Next Create SpokeVm with SpokeVnet and its subnet.

Home > Network foundation | Virtual network

Create virtual network

Basics Security IP addresses Tags

+ Add a subnet

10.0.0.0/16
10.0.0.0
10.0.0.0 - 10.0.255.255

Subnets	IP address
Usubnet	10.0.0.0 -

Add IPv4 address space

Previous Next Review Add Cancel

Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add sele

Subnet purpose ⓘ Azure Firewall

Name * ⓘ AzureFirewallSubnet

IPv4

Include an IPv4 address space ☒

IPv4 address range ⓘ 10.0.0.0/16
10.0.0.0 - 10.0.255.255

Starting address * ⓘ 10.0.1.0

Size ⓘ /26 (64 addresses)

Subnet address range ⓘ 10.0.1.0 - 10.0.1.63

IPv6

Include an IPv6 address space ☐ This virtual network has no IPv6 address ranges.

Private subnet

Create virtual network

Validation passed

Basics Security IP addresses Tags Review + create

Subscription	Azure subscription 1
Resource Group	Ufirewall-rg
Name	Ufirewall-Vnet
Region	Italy North
Security	
Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled
IP addresses	
Address space	10.0.0.0/16 (65,536 addresses)
Subnet	Usubnet (10.0.0.0/24) (256 addresses)
Subnet	AzureFirewallSubnet (10.0.1.0/26) (64 addresses)

Previous Next Create Download a template for automation

✓ Now lets Create Firewall

Create a firewall ...

Subscription *	Azure subscription 1
Resource group *	Ufirewall-rg
	Create new
Instance details	
Name *	Ufirewall01
Region *	Italy North
Availability zone ⓘ	None
Firewall SKU	<input type="radio"/> Basic
	<input checked="" type="radio"/> Standard
	<input type="radio"/> Premium

Create a firewall ...

Firewall management	<input type="radio"/> Use a Firewall Policy to manage this firewall
	<input checked="" type="radio"/> Use Firewall rules (classic) to manage this firewall
Choose a virtual network	<input type="radio"/> Create new
	<input checked="" type="radio"/> Use existing
Virtual network	Ufirewall-Vnet (Ufirewall-rg)
Public IP address *	(New) Ufirewall-pip
	Add new

Firewall Management NIC

Firewall Management NIC separates Firewall management traffic from customer traffic. A dedicated subnet is required with its own associated public IP address that will be used exclusively by the Azure platform and can't be used for any other purpose.

Enable Firewall Management NIC	<input type="checkbox"/>
	 Critical Firewall features such as Forced Tunneling and Packet Capture require management NIC to be enabled.

[Previous](#) | [Next : Tags >](#) | [Download a template for automation](#)



✓ Next create SpokeVm in same region and give its subnet.

Create a virtual machine



Help me create a low cost VM

Validation passed



Help me create a low cost VM

Help me create a VM optimized for high availability

Subscription	Azure subscription 1
Resource group	(new) Uspoke-rg
Virtual machine name	Uspoke-vm
Region	Italy North
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Standard
Image	Windows Server 2025 Datacenter - Gen2
VM architecture	x64
Size	Standard D2ads v5 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Networking

Virtual network	vnet-italynorth
Subnet	snet-italynorth-1
Public IP	(new) Uspoke-vm-ip
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled



Uspoke-vm

Virtual machine



Help me copy this VM in any region

Manage this VM with Azure CLI

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Connect

Networking

Settings

Availability + scale

Security

Uspoke-vm virtual machine agent status is not ready. Troubleshoot the issue →



Help me copy this VM in any region



Connect



Start



Restart



Stop



Hibernate



Capture



Delete



Refresh



Scale



Open in mobile



Feedback

Essentials

Resource group [\(move\)](#) : Uspoke-rg

Status : Running

Location : Italy North

Subscription [\(move\)](#) : Azure subscription 1

Subscription ID : 5d75b66d-66bf-44e0-8d7e-7e61e4b043d7

Operating system : Windows

Size : Standard D2ads v5 (2 vcpus, 8 GiB memory)

Primary NIC public IP : [172.213.227.14](#)
[1 associated public IPs](#)

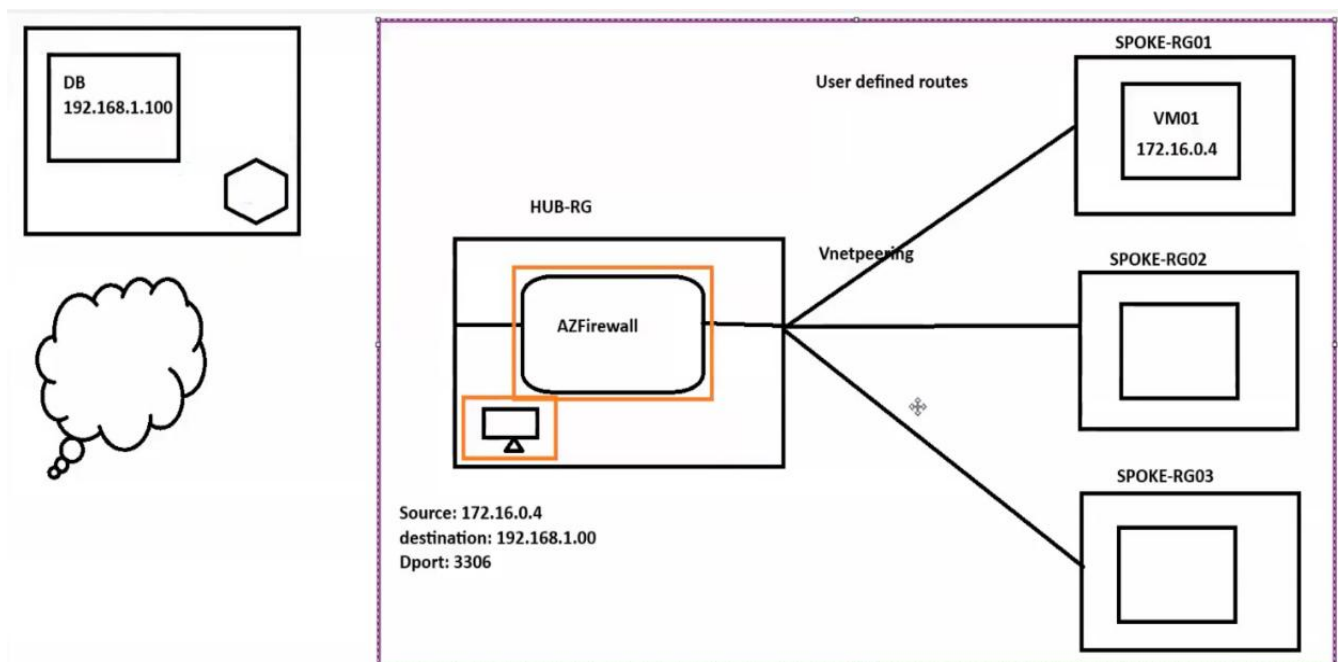
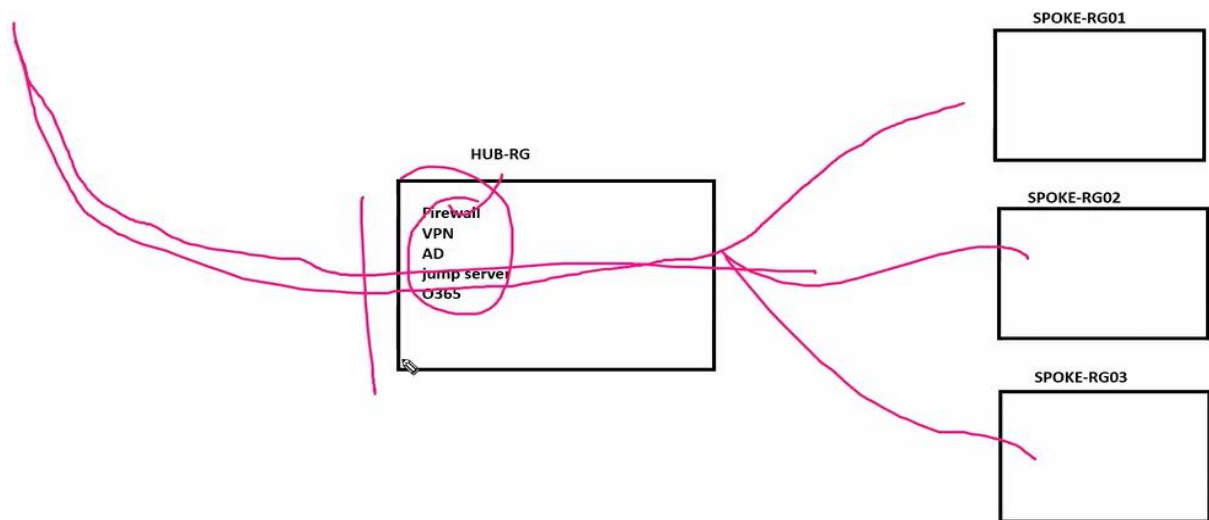
Virtual network/subnet : [vnet-italynorth/snet-italynorth-1](#)

DNS name : [Not configured](#)

Health state : -

Time created : 13/02/2026, 10:24 UTC

HUB & Spoke Architecture



- ✓ Machines behind the firewall, by default there will be denied rule we can't access the machines
- ✓ From public even though machines have public Ip once the machine is behind the firewall by default traffic will be blocked.
- ✓ For now, we created Firewall and Spokevm (windows)
- ✓ Let's log into spokevm(pip)
- ✓ Next Lets config Vnet peering from firewallVnet & SpokeVnet

✓ We see two diff Vnet for firewall and spoke below

Network foundation | Virtual networks

Preview

Search

Overview

Virtual network

Virtual Network overview

Virtual networks

NAT gateways

Public IP addresses

Network interfaces

Network security

Create Manage view Refresh Export to CSV Open query Assign tags Add to service gr

Filter for any field...

Subscription equals all Resource Group equals all Location equals all

Name ↑	Resource Group	Location
<input checked="" type="checkbox"/> Ufirewall-Vnet	Ufirewall-rg	Italy North
<input type="checkbox"/> VFirewallnet	VFIREWALLRG1	South Africa North
<input type="checkbox"/> vnet-canadacentral	VSPOKE-RG1	Canada Central
<input type="checkbox"/> vnet-centralindia	BH-rg	Central India
<input checked="" type="checkbox"/> vnet-italynorth	Uspoke-rg	Italy North

✓ Choose any Vnet for peering

Ufirewall-Vnet | Peerings

Virtual network

Search

Peerings

Service endpoints

Private endpoints

Properties

Locks

Add Refresh Export to CSV Delete Sync

Virtual network peering enables you to seamlessly connect two or more v

Filter by name...

Showing all 0 items

Name ↑ Peering

Add peering

Ufirewall-Vnet

Remote virtual network summary

Peering link name * firewall-to-spoke

I know my resource ID ☐

Subscription * Azure subscription 1

Virtual network * vnet-italynorth (Uspoke-rg)

Remote virtual network peering settings

Allow 'vnet-italynorth' to access 'Ufirewall-Vnet' ☒

Allow 'vnet-italynorth' to receive forwarded traffic from 'Ufirewall-Vnet' ☐

Allow gateway or route server in 'vnet-italynorth' to forward traffic to 'Ufirewall-Vnet' ☐

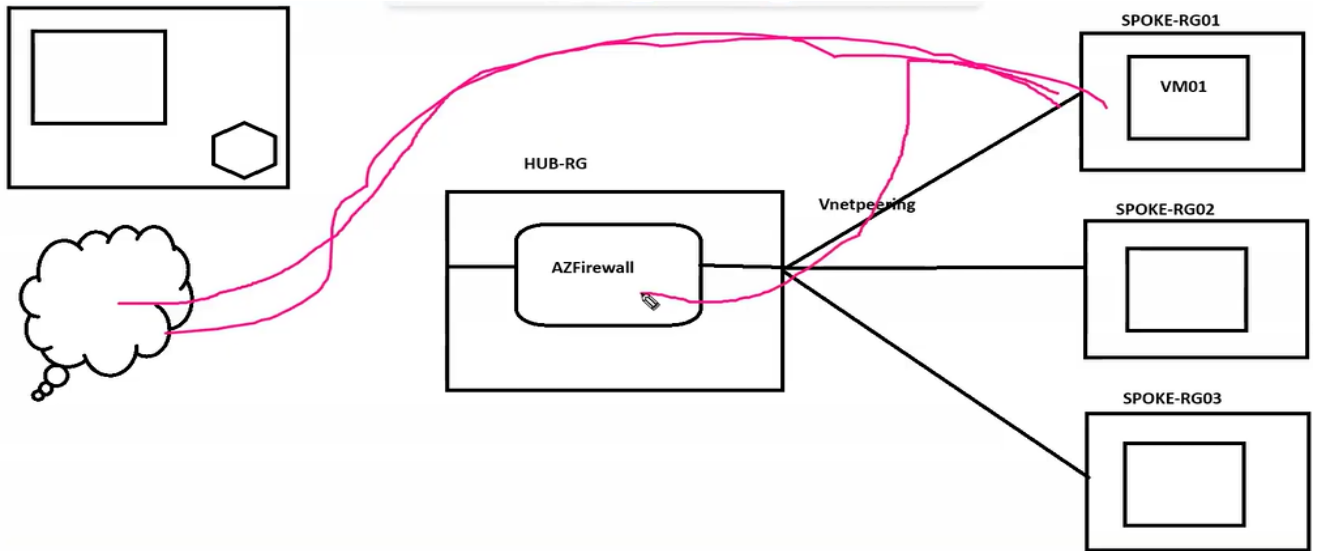
Enable 'vnet-italynorth' to use 'Ufirewall-Vnet's' remote gateway or route server ☐

Local virtual network summary

Peering link name * spoke-to-firewall

Add Cancel

- ✓ After Vnet peering we can still connect to spokeVm bcz the traffic is going through outside and connecting to spokeVm.



- ✓ Let's Redirect traffic to firewall
- ✓ For that use should right **Route Table (User Defined Routes)**
- ✓ Search for Route Tables and click on Create

Create Route Table ...

Basics Tags Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like to manage all your resources.

Subscription * ⓘ

[Create new](#)

Instance details

Name * ⓘ

Propagate gateway routes * ⓘ ☐ Yes ☐ No

Region * ⓘ

✓ Below click on Add and add route

UspokeRT | Routes ☆ ...
Route table

Search

+ Add Refresh Give feedback

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Routes

Subnets

Search routes

Name ↑↓	Address prefix
No results.	

Home > RouteTableDeployment-1770984473171 | Overview > UspokeRT

UspokeRT | Routes ☆ ...
Route table

Search

+ Add Refresh Give feedback

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Configuration

Routes

Subnets

Properties

Locks

Monitoring

Search routes

Name ↑↓	Address prefix
No results.	

Add route

UspokeRT

Route name *
To_Firewall

Destination type * ⓘ
IP Addresses

Destination IP addresses/CIDR ranges * ⓘ
0.0.0.0/0

Next hop type * ⓘ
Virtual appliance

Next hop address * ⓘ
10.0.1.4

Add

✓ **0.0.0.0/0** is Any above. Copy below **Firewall Private Ip** Below

Ufirewall01 ☆ ☆ ...
Firewall

Show the latest IDPS hits for this firewall How to protect my firewall against failures Che

Search

Migrate to firewall policy Delete Lock Change SKU

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

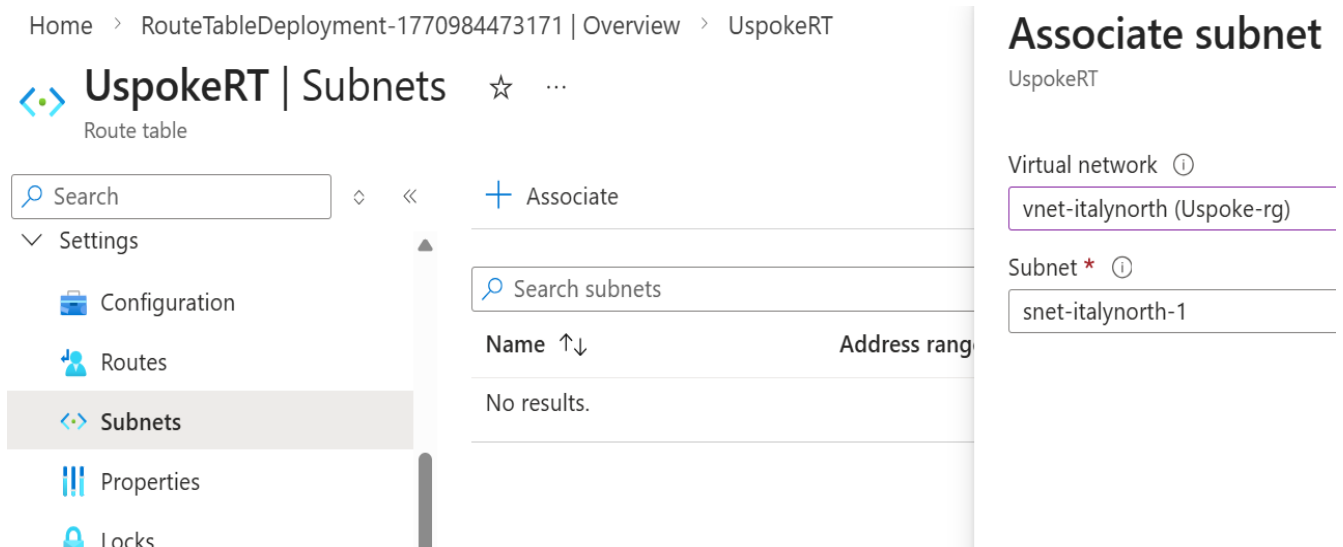
Settings

For advanced security protection of your network, you can easily upgrade to Azure Firewall Premium

Resource group (move) Ufirewall-rg	SKU Standard(change)
Location Italy North	Subnet AzureFirewallSubnet
Subscription (move) Azure subscription 1	Public IP Ufirewall01 Copied
Subscription ID 5d75b66d-66bf-44e0-8d7e-7e61e4b043d7	Private IP 10.0.1.4

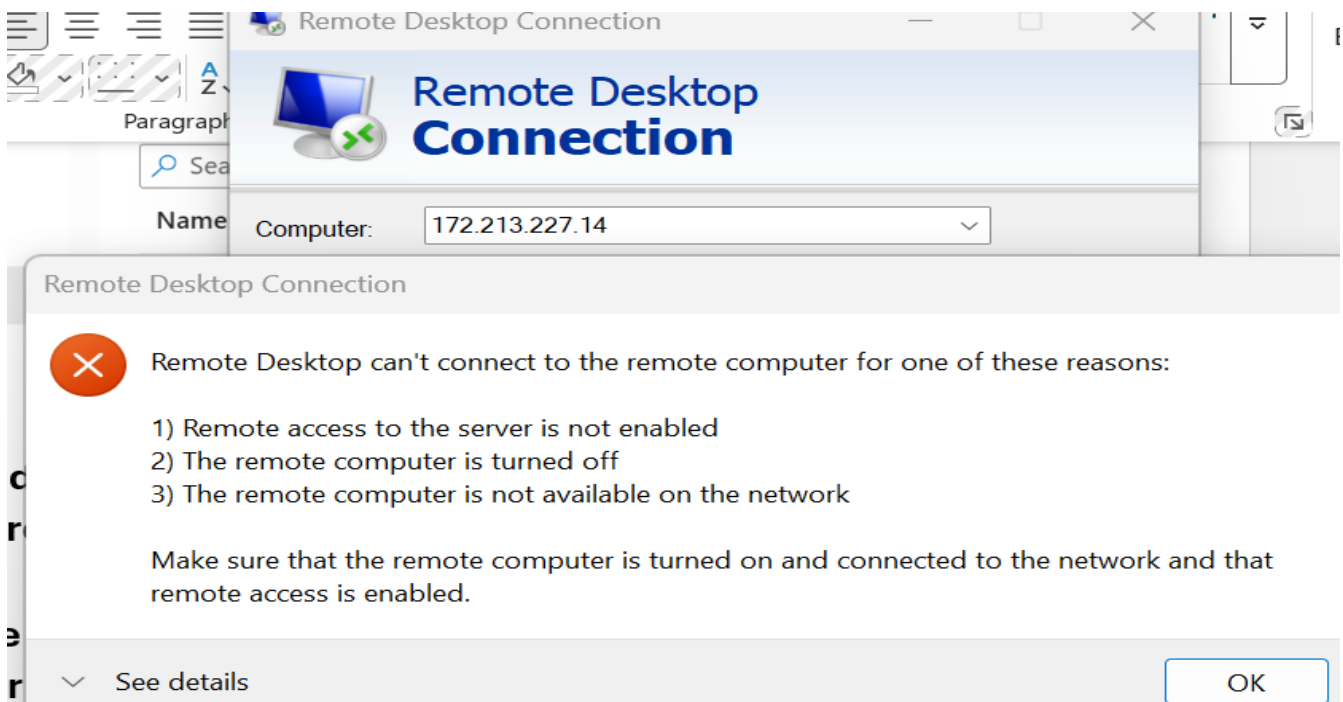
✓ Now from SpokeVm whatever the traffic it should hit firewall first

➤ Now Next Once We Write the **Route rule it should be attached to Subnet**

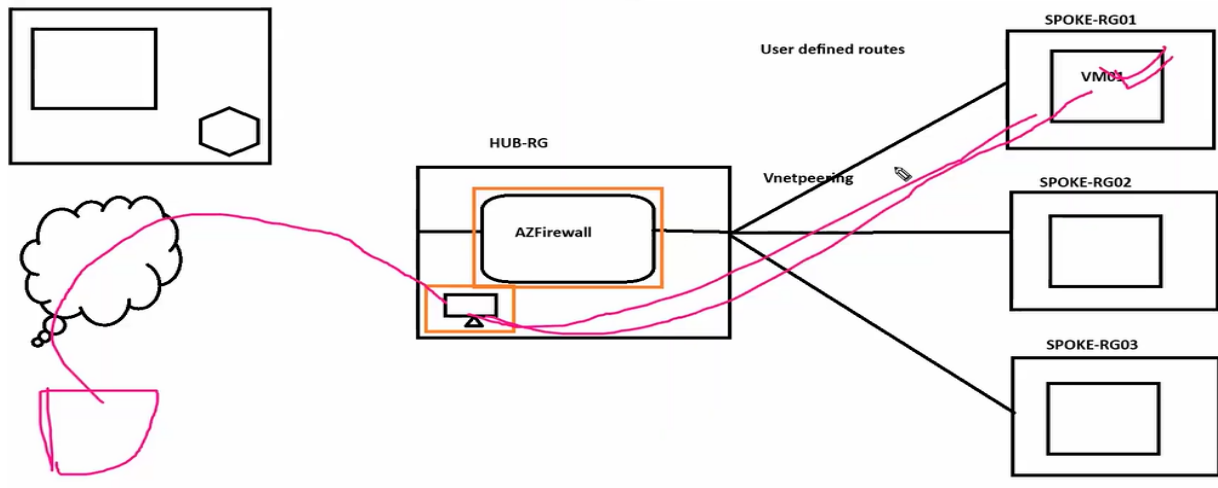


✓ We have defined Routing, so the traffic coming from inside it should use Azure Firewall only, the traffic will flow from firewall only.

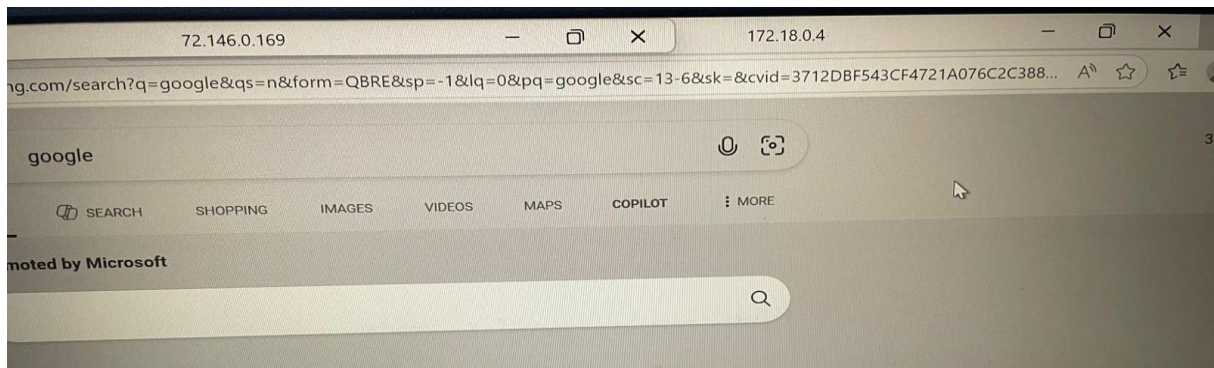
✓ After adding the rules to subnet automatically SpokeVM which is logged in earlier it will disconnect, Bcz traffic Diverted from firewall.



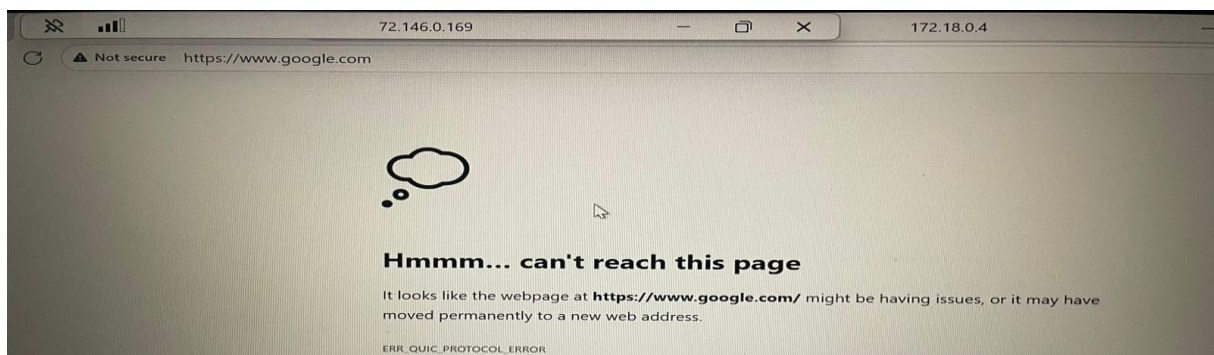
- Next create **another VM** using **subnet** in **FirewallVnet**.
- This VM just to know what's happening in SpokeVM.
- To access this from my **LAPTOP** → **VM** → **SPOKEVM**





- ✓ Let's create **VM (windows)** on **HUB-RG(FirewallVnet)**
- ✓ Now Connect to this VM using **PublicIP(72.146.0.169)** on RDC
- ✓ After connecting to VM, open RDC in it and **Connect** to SpokeVM **internally** by using **SpokeVM PrivateIP(172.18.0.4)**



- ✓ We can't access anything bcz internet is not allowed and rules not match on firewall and this is behind the firewall.



❖ Let's talk about Rules (follow below steps)

 **Network security | Azure Firewall Policies** ...  Identify policies imp

Preview

⌵ ⌵

[+ Create](#) [⚙️ Manage view](#) ⌵ [🔄 Refresh](#) [⬇️ Export to CSV](#)

[🔍 Filter for any field...](#) [Subscription equals all](#) [Resou](#)

[🛡️ Overview](#)

[📁 Firewall Manager](#)

[🛡️ Azure Firewalls](#)

[🛡️ Azure Firewall Policies](#)

[➤ WAF + DDoS](#)

[➤ Secure your resources](#)

Create an Azure Firewall Policy ...

[basics](#) [DNS Settings](#) [TLS inspection](#) [Rules](#) [IDPS](#) [Threat intelligence](#) [Tags](#) [Review + create](#)

Define network and application level rules for traffic filtering across multiple Azure Firewall instances in Secured Virtual Hut

Project details

Subscription *

Azure subscription 1

Resource group *

Ufirewall-rg
[Create new](#)


Policy details

Name *

defaultpolicy

Region *

Italy North

 Parent policy must be in the same region as child policy. Firewall policy can be associated with Firewalls across regions regard

Your new policy will inherit all rule collections from the selected parent policy below. Rule collections inherited from the pa

Policy tier

☐ Basic

☒ Standard


☐ Premium

Parent policy ⓘ

None

[Review + create](#) [Previous](#) [Next : DNS Settings >](#) [Download a template for automation](#)

Create an Azure Firewall Policy ...

 Validation passed

[Basics](#) [DNS Settings](#) [TLS inspection](#) [Rules](#) [IDPS](#) [Threat intelligence](#) [Tags](#) [Review + create](#)

Summary

[Basics](#)

Subscription

Resource group

Name

Region

Policy tier

Azure subscription 1

Ufirewall-rg

defaultpolicy

Italy North

Standard

[Rules](#)

Parent policy

Rule collections

None

RULE COLLECTION TYPE

No results



Microsoft.FirewallPolicy-20260213212221 | Overview

Deployment

Search



Delete



Cancel



Redeploy



Download



Refresh



Overview



Inputs



Outputs



Template



Your deployment is complete



Deployment name : Microsoft.FirewallPolicy-20260213212221

Subscription : [Azure subscription 1](#)

Resource group : [Ufirewall-rg](#)



Deployment details



Next steps

[Go to resource](#)

- ✓ Created Name(**defaultpolicy**) but we didn't added rules in it, let's do that.



defaultpolicy

Firewall Policy



Search



Resource visualizer



Management



Rules



Rule collections



DNAT rules



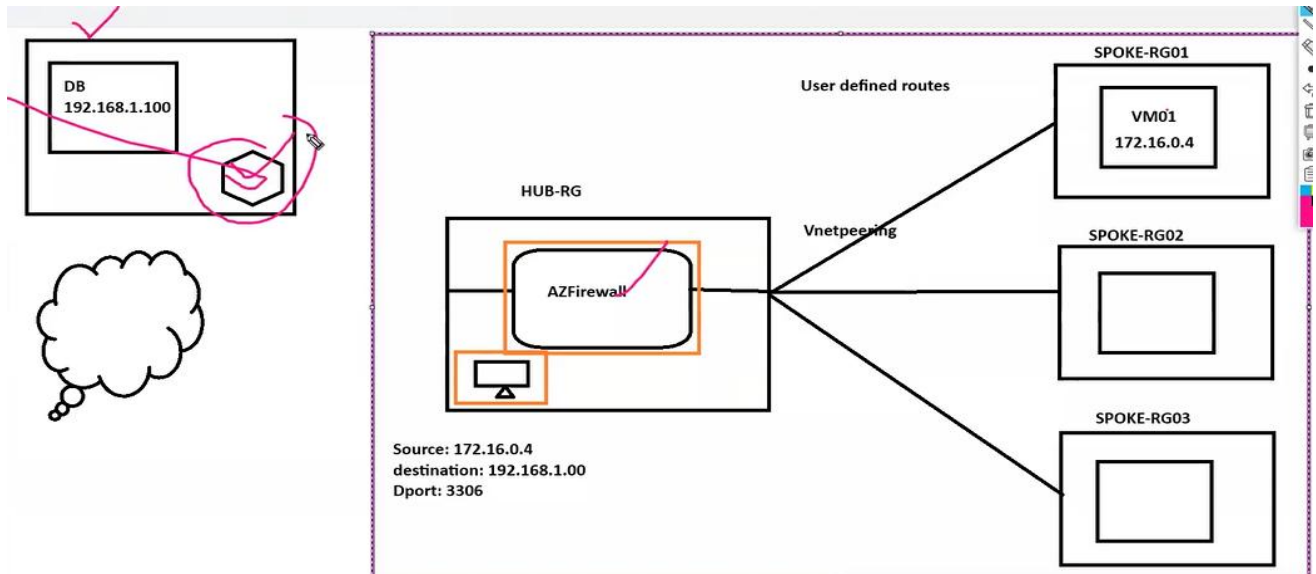
Network rules



Application rules

- ✓ **Network rule** if we want to allow **IP to IP** then we use it.
- ✓ We don't use domain names here
 - Below you can see example which we used in lab.

- ✓ App & DB in different datacentres and they both have firewalls and both should config firewall rules then only we can access both.



Home > Microsoft.FirewallPolicy-2015-08-01 | defaultpolicy | Network Firewall Policy

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Resource visualizer
- Management
- Rules
 - Rule collections
 - DNAT rules
 - Network rules
 - Application rules

Add a rule collection

Name * Allow_DB ✓

Rule collection type * Network ✓

Priority * 100 ✓

Rule collection action Allow ✓

Rule collection group * DefaultNetworkRuleCollectionGroup ✓

Rules

Name *	Source type	Source	Protocol *	Destination Ports *	Destination Type *	Destination *
Allow_DB ✓	IP Address ✓	* ✓	0 selected ✓	3306 ✓	IP Address ✓	192.168.1.100 ✓
	IP Address	*, 192.168.10.1, 192...	0 selected	80,8000-9000	IP Address	*,10.0.0.1,10.1.0.0/1...

❖ Application rules

defaultpolicy | Application rules ☆ ...

Search

+ Add a rule collection + Add rule Edit Delete

Rules

- Rule collections
- DNAT rules
- Network rules
- Application rules

Rules are shown in the order of execution below. Network rules take prec over rule collection group priority and rule collection priority.

Search to filter items...

Rule Collection P...↑↓	Rule collection n...	Rule name
No application rule collections found		

Home > Microsoft.FirewallPolicy-20260213

defaultpolicy | Application Firewall Policy

Search

- Rules
 - Rule collections
 - DNAT rules
 - Network rules
 - Application rules**
- Settings
 - Parent policy
 - DNS
 - Threat Intelligence

Add a rule collection

Name *

Rule collection type *

Priority *

Rule collection action

Rule collection group *

Rules

Name *	Source type	Source	Protocol *	TLS inspection	Destination Type *	Destination *
Allow_google	IP Address	*	http,https	<input type="checkbox"/> TLS inspection	FQDN	*.google.com
Allow_yahoo	IP Address	*	http,https	<input type="checkbox"/> TLS inspection	FQDN	*.yahoo.com

✓ **Associate this defaultpolicy to your Firewall**

✓ **Go to firewall→Migrate to firewall policy→Attach an existing firewall policy below**

Home > Network security | Azure Firewalls

Ufirewall01

Firewall

Search

- Overview**
- Activity log
- Access control (IAM)

Migrate to firewall policy

Attach an existing firewall policy

Selected Firewall Policy will override the current policy and rules on the firewall

Firewall Policy	Inherits From	Firewall Policy Tier	Subscription	Resource Group
<input checked="" type="checkbox"/> defaultpolicy		Standard	Azure subscription 1	Ufirewall-rg

✓ **Select above policy and save.**

❖ DNAT rules

- ✓ Below I want to connect from internet to backend machine.
- ✓ Like from My laptop to directly Backend machine, but we can't connect bcz the machine is behind the firewall.
- ✓ But in this case, we can cannot by use Firewall Public IP
- ✓ Outside traffic hits to Firewall Public IP from that traffic will go to Backend machine, here Backend Private IP masked by firewall.
- ✓ Firewall PublicIP (172.213.217.109)→Backend SpokeVM PrivateIP (172.18.0.4)
- ✓ Same with ports 50000→3389
- ✓ Translating with Public→Private and from Port→Port for Security to Machine, we are just Mapping with one to one.
- ✓ We can choose servers; on those we can add this Mapping at in emergency situations then access backend machines.

Home > Microsoft.FirewallPolicy-20260213

defaultpolicy | DNAT r

Firewall Policy

Search

Rules

Rule collections

DNAT rules

Network rules

Application rules

Settings

Parent policy

DNS

Add a rule collection

Name * Dnatrule ✓

Rule collection type * DNAT ✓

Priority * 100 ✓

Rule collection action Destination Network Address Translation (DNAT) ✓

Rule collection group * DefaultDnatRuleCollectionGroup ✓

Rules

Source	Protocol *	Destination Ports *	Destination (Firewall IP)	Translated type *	Translated address or	Translated p
*	TCP ✓	50000 ✓	172.213.217.109 ✓	IP Address ✓	172.18.0.4 ✓	3389 ✓

Example Below:

Protocol *	Destination Ports *	Destination (Firewall IP)	Translated type *	Translated address or	Translated port *
TCP	50000	20.172.146.62	IP Address	172.16.0.4	3389
	50001	20.172.146.62		172.16.0.5	3389
	50002	20.172.146.62		172.16.0.6	3389

- ✚ There is another option DNATTING→we connect with Private IPs only by using VPS, we can login into the azure infrastructure to one of the gem servers from there we are going to connect.

✓ Copy **firewallPublicIP:50000**

✓ By this we can connect to Backend SpokeVM

